UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/669,784	09/24/2003	James C. Farmer	10002762-3	6401

7590 05/23/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
TSAI, SHENG JEN	
ART UNIT	PAPER NUMBER
2186	
MAIL DATE	DELIVERY MODE
05/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/669,784	FARMER ET AL.	
	Examiner	Art Unit	
	SHENG-JEN TSAI	2186	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,8-13,15,16,19 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,8-13,15,16,19 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is taken in response to Applicants' Amendments and Remarks filed on February 1, 2008 regarding application 10/669,784 filed on September 24, 2003.

2. Claims 2, 6-7, 14 and 17-18 have been cancelled.

Claims 1, 8 and 15 have been amended.

Claims 1, 3-5, 8-13, 15-16 and 19-20 are pending under consideration.

3. ***Response to Amendments and Remarks***

Applicants' amendments and remarks have been fully and carefully considered, with the Examiner's response set forth below.

(1) In view of Applicants' clarification and explanation on the subject matter of "computer readable medium," the objection to the Specification as failing to provide proper antecedent basis for the claimed subject matter of claim 15 has been withdrawn. However, it is understood and agreed that the scope of the "computer readable medium" is defined as memory type of storage devices, such as "read only memory" or "random access memory."

(2) Applicants amended independent claims 1 and 15 with the additional limitation of "based on a portion of said user data," and contended that Carcia (US 6,151,689) in view of Weber (US 6,212,610) fails to teach "said key data being generated based upon a destination address of said write operation and base on a portion of user data."

In response, a new reference (Taguchi et al., US 5,915,025) that explicitly teach the amended new limitation has been identified, and a new ground of claim analysis based on Carcia in view of Taguchi has been made. Refer to the corresponding sections of the following claim analysis for details.

(8) Applicants amended independent claim 8 with the additional limitation of "based on a portion of said user data," and contended that Carcia (US 6,151,689) in view of Adler (US 4,255,811) fails to teach "said key data being generated based upon a system clock setting of said computer system and base on a portion of user data."

Particularly, Applicants contend that the Adler reference fails to teach the key is generated based on a portion of user data as currently claimed.

However, it is noted that the Carcia reference explicitly teaches generating key using user data [the corresponding key data in Carcia's invention is the CRC data, which is generated using user data -- Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, …" (column 31, lines 10-25); Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15].

Thus, the combination of Carcia and Adler teaches the cited limitation because Carcia teaches generating key data using user data and Adler teaches generating key data using system clock setting.

4. ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1,3-5, 15-16 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garcia et al. (US 6,151,689, hereinafter referred to as Garcia), and in view of Taguchi et al. (US 5,915,025, hereinafter referred to as Taguchi).

It is noted that, in the following claim analysis, those elements recited by the claims are presented using **bold** font.

As to claim 1, Garcia discloses **a method for protecting memory space in a target storage device during a write operation in a computer system** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)], **the method comprising**:

creating a single data packet [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC], **including user data** [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC] **that is to be written in a write operation to said target storage device** [figure 6, 24b is the target storage device] **and key data** [for example, the CRC may be the corresponding key data; Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, …" (column 31, lines 10-25)] **that is used to establish authorization to store said user data** [Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15]; **said key data being generated based upon a destination address of said write operation** [this limitation is taught by Taguchi, see below] **and based on a portion of said user data** [the corresponding key data in Carcia's invention is the CRC data, which is generated using user data -- Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, …" (column 31, lines 10-25); Use of CRC in this manner operates to protect message packets from end to end because the router elements do not

modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches “access validation” in details from column 30, lines 56 through column 37, lines15; Taguchi also teaches generating key data using user data -- encryption key generation means for generating an encryption key depending on an attribute of data including instructions to be encrypted; decryption key generation means for generating a decryption key depending on an attribute of encrypted data (col. 26, lines 15-20)];

transmitting said single data packet to the target storage device [see figure 6];

determining whether said key data is valid [If the received message packet is found to have a bad CRC (or it is tagged with a "This Packet Bad" (TPB) command symbol, see below) the packet is discarded, and access is denied (column 31, lines 22-25)];

writing said user data into said target storage device only when said key data is valid [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

Regarding claim 1, Garcia teaches using CRC, which is generated from user data, as a key to establish authorization to store data, and does not teach that said key data being generated based upon a destination address of said write operation.

Taguchi teaches in the invention "Data Processing Apparatus with Software Protecting Functions" a mechanism for memory access protection [abstract] in which the key data is generated based upon a destination address [figure 15 shows that the key to be used depends on the page number; figure 16 shows that the key to be used depends on the address tag; figure 17; A data processing apparatus with software protecting functions according to claim 1, wherein said encryption key generation means generates said encryption key depending on either an address or an address region of data to be encrypted; and wherein said decryption key generation means generates said decryption key depending on either said address or said address region of the encrypted data (col. 26, lines 36-44)] and based upon a portion of said user data [encryption key generation means for generating an encryption key depending on an attribute of data including instructions to be encrypted; decryption key generation means for generating a decryption key depending on an attribute of encrypted data (col. 26, lines 15-20)].

Taguchi also teaches that the motivation of using a key that is generated based on the destination address as well as user data is because it raises the level of protection, requires very little hardware storage, and can cover an unlimited number of memory areas [column 3, lines 56-62].

Therefore, it would have been obvious for one of ordinary skills in the art at the time of Applicants' invention to protect memory by using a key that is generated based on the destination address as well as user data, as demonstrated by Taguchi, and to incorporate it into the existing scheme disclosed by Garcia, because it offers the

advantages of raising the level of protection, requiring very little hardware storage, and covering an unlimited number of memory areas.

As to claim 3, Garcia teaches that **the method of claim 1 further comprising: performing a Boolean operation on selected bits of said user data to generate said key data** [for example, the CRC may be the corresponding key data, which is calculated based on Boolean operations on Data bits].

As to claim 4, Garcia teaches that **the method of claim 1 further comprising**: **generating verification data from said user data at a controller of said target storage device** [Error-checking of the communication flow between the components of the processing system is achieved by adding a cyclic-redundancy-check (CRC) to the message packets that are sent between the elements of the system (column 5, lines 28-31)]; **and**

comparing said key data in said single data packet with said verification data to determine if said key data matches said verification data [The CRC of each message packet is checked not only at the destination of the message, but also while en route to the destination by each router element used to route the message packet from its source to the destination. If a message packet is found by a router element to have an incorrect CRC, the message packet is tagged as such, and reported to a maintenance diagnostic system (column 5, lines 31-40)].

As to claim 5, Garcia teaches that **the method of claim 4 further comprising: storing said user data to said target storage device if said key data matches said verification data** [CPUs and I/O devices may write to, or read from, memory of a CPU

of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

As to claim 15, it recites substantially the same limitations as in claim 1, and is rejected for the same reasons set forth in the analysis of claim 1. Refer to "As to claim 1" presented earlier in this Office Action for details. Note that Taguchi teaches that said key data is generated based on a destination address as explained in "As to claim 1."

As to claim 16, it recites substantially the same limitations as in claim 5, and is rejected for the same reasons set forth in the analysis of claim 5. Refer to "As to claim 5" presented earlier in this Office Action for details.

As to claim 19, it recites substantially the same limitations as in claim 4, and is rejected for the same reasons set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this Office Action for details.

As to claim 20, it recites substantially the same limitations as in claim 4, and is rejected for the same reasons set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this Office Action for details. Also see figure 6 of Garcia et al.

6. Claims 8-13, 15-16 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garcia et al. (US 6,151,689, hereinafter referred to as Garcia), and in view of Adler (US 4,255,811).

As to claim 8, Garcia discloses **a system for conducting a protected memory write to a target storage device in a single transaction within a computer system**

[CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract); figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC], **the system comprising**:

Means for simultaneously delivering user data and key data to a controller of said storage device, wherein said user data is to be written to said storage device [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, data and CRC; figure 6, 24b is the target storage device] **and key data** [for example, the CRC may be the corresponding key data; Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, …" (column 31, lines 10-25)] **is used to establish authorization to store said user data** [Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15]; **said key data being generated based upon a system clock setting of said computer system** [this limitation is taught by Adler, see below]; **and based on a portion of said**

user data [the corresponding key data in Carcia's invention is the CRC data, which is generated using user data -- Accesses to the memory 28 are validated by the AVT logic 90 of each interface unit 24 (FIG. 5), using all of six checks: (1) that the CRC of the message packet carrying the request is error free, …" (column 31, lines 10-25); Use of CRC in this manner operates to protect message packets from end to end because the router elements do not modify or regenerate the CRC as the message packet passes through. The CRC of each message packet is checked at each router crossing. A command symbol--"This packet Good" (TPG) or "This Packet Bad" (TPB)--is appended to every packet (column 5, lines 39-45); Garcia further teaches "access validation" in details from column 30, lines 56 through column 37, lines15]; **and Means for determining whether said key data authorizes writing said user data to said storage device** [If the received message packet is found to have a bad CRC (or it is tagged with a "This Packet Bad" (TPB) command symbol, see below) the packet is discarded, and access is denied (column 31, lines 22-25); CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

Regarding claim 8, Garcia teaches using CRC, which is generated from user data, as a key to establish authorization to store data, and does not teach that said key data being generated based upon a system clock setting of said computer system.

Adler teaches in the invention "Key Controlled Block Cipher Cryptographic System" a mechanism for memory access protection in which a valid key is required to be granted access right to certain pages of a memory [All authorized subscribers who are permitted access to data within the network are assigned a unique key consisting of a combination of binary symbols. The central processing unit within the computing network contains a complete listing of all distributed authorized subscriber keys. All communications transmitted from terminal input are encrypted into a block cipher by use of the cryptographic system operating under the control of the subscriber key which is inputed to the terminal device. At the receiving station or central processing unit, an identical subscriber key which is obtained from internal tables stored within the computing system is used to decipher all received ciphered communications (abstract)].

Specifically, Adler teaches that a key is generated based on a system clock setting of said computer system [figure 4 shows "key generation clock" being used to generate keys; The second is the key generation clock K which controls the operation of the key generation shift registers shown in FIGS. 3A and 3B which sequentially generate the key material for each of the rounds (column 6, lines 7-11); column 6, lines 1-21].

Adler also teaches that the motivation of using a key that is generated based on a system clock setting of said computer system is because it allows generation of keys of great cryptographic strength by iterating the algorithm many more rounds than practically possible [column 14, lines 46-53].

Therefore, it would have been obvious for one of ordinary skills in the art at the time of Applicants' invention to protect memory by using a key that is generated based on a system clock setting of said computer system, as demonstrated by Adler, and to incorporate it into the existing scheme disclosed by Garcia, because it allows generation of keys of great cryptographic strength by iterating the algorithm many more rounds than practically possible.

As to claim 9, Garcia teaches that **the system of claim 8 further comprising: means for writing said user data to said target storage device only when said key data authorizes writing said user data** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

As to claim 10, Garcia teaches that **the system of claim 8 further comprising: means, at an originating device, for calculating said key data using an algorithm before said user data and said key data is sent to said storage device** [figures 3A~3D and 4A~4C show various types of packets, comprising Header, Address, Data and CRC, and CRC is calculated using Data; If the received message packet is found to have a bad CRC (or it is tagged with a "This Packet Bad" (TPB) command symbol, see below) the packet is discarded, and access is denied (column 31, lines 22-25)].

As to claim 11, Garcia teaches that **the system of claim 10 wherein said algorithm calculates said key data from said user data** [figures 3A~3D and 4A~4C

show various types of packets, comprising Header, Address, Data and CRC, and CRC is calculated using Data].

As to claim 12, Garcia teaches that **the system of claim 8 further comprising**: **Means for generating verification data at said target storage device controller** [Error-checking of the communication flow between the components of the processing system is achieved by adding a cyclic-redundancy-check (CRC) to the message packets that are sent between the elements of the system (column 5, lines 28-31)]; **and**

Means for comparing said verification data to said key data [The CRC of each message packet is checked not only at the destination of the message, but also while en route to the destination by each router element used to route the message packet from its source to the destination. If a message packet is found by a router element to have an incorrect CRC, the message packet is tagged as such, and reported to a maintenance diagnostic system (column 5, lines 31-40)].

As to claim 13, Garcia teaches that **the system of claim 8 wherein said determining means further comprising: means for authorizing writing of said user data only where said verification data matches said key data** [CPUs and I/O devices may write to, or read from, memory of a CPU of the system. Memory protection is provided by an access validation method maintained by each CPU in which CPUs and/or I/O devices are provided with a validation to read/write memory of that CPU, without which memory access is denied (abstract)].

As to claim 15, it recites substantially the same limitations as in claim 8, and is rejected for the same reasons set forth in the analysis of claim 8. Refer to "As to claim 8" presented earlier in this Office Action for details. Note that Alder teaches that said key data is generated based on a system clock setting of said computer system as explained in "As to claim 8."

As to claim 16, it recites substantially the same limitations as in claim 5, and is rejected for the same reasons set forth in the analysis of claim 5. Refer to "As to claim 5" presented earlier in this Office Action for details.

As to claim 19, it recites substantially the same limitations as in claim 4, and is rejected for the same reasons set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this Office Action for details.

As to claim 20, it recites substantially the same limitations as in claim 4, and is rejected for the same reasons set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this Office Action for details. Also see figure 6 of Garcia et al.

Conclusion

7. Claims 1, 3-5, 8-13, 15-16 and 19-20 are rejected as explained above.

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sheng-Jen Tsai whose telephone number is 571-272-4244. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matthew Kim can be reached on 571-272-4182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Sheng-Jen Tsai/

Partial Signatory Examiner, Art Unit 2186

May 21, 2008

/Matt Kim/

Supervisory Patent Examiner, Art Unit 2186